UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/647,644	08/25/2003	Mark Eric Obrecht	6002-00602	2528

35690 7590 03/07/2008

MEYERTONS, HOOD, KIVLIN, KOWERT & GOETZEL, P.C.
P.O. BOX 398
AUSTIN, TX 78767-0398

EXAMINER	
SHERKAT, AREZOO	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
03/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/647,644	OBRECHT ET AL.	
	Examiner	Art Unit	
	AREZOO SHERKAT	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 February 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *105-107,109-118 and 127-167* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *105-107,109-118,and 127-167-* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment received on 2/11/2008. Claims 1-104, 108, and 119-126 are cancelled. Claims 105-107, 109-118, and 127-167 remain pending.

Response to Arguments

Applicant's arguments, see Remarks, filed 2/11/2008, with respect to the rejection(s) of claim(s) 105-107, 109-118, and 127-167 under 35 U.S.C 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Muttik, (U.S. Patent No. 6,775,780), Chess et al., (U.S. Patent No. 6,772,346), and Kouznetsov, (U.S. Patent No. 6,973,577).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 105-107, 115-118, and 127-129, 132, 134-139, 141-143, 145, 147-148, 150-159, and 162-167 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Muttik, (U.S. Patent No. 6,775,780), in view of Chess et al., (U.S. Patent No. 6,772,346 and Chess hereinafter).

Regarding claims 105-107, 115, 117, 127-128, 151-152, 159, and 167, Muttik discloses a computer-implemented method comprising:

selecting an active program on a computer system as code under investigation (col. 3, lines 23-52), and executing malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a plurality of detection routines (i.e., comparison unit can include any type of mechanism that can compare system calls 220-222 against profiles of system calls made by malicious programs, wherein comparison unit takes as input a set of rules 210 and a set of profiles of system call patterns malicious programs from database 206)(col. 3, lines 54-67 and col. 4, lines 1-24), wherein said executing includes:

applying the plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results, weighting each of the first plurality of results to obtain a first score (i.e., negative weight) indicative of whether the code under investigation has characteristics and/or behaviors typically associated with valid code (i.e., weights can be negative for activities which is more likely to be present in non-malicious code)(col. 5, lines 15-17);

applying the plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results, weighting each of the second plurality of results to obtain a second score (i.e., positive weight) indicative of

whether the code under investigation has characteristics and/or behaviors typically associated with malicious code, wherein the second score is obtained independently of the first score (i.e., weights can be positive for suspicious/malicious activities)(col. 5, lines 15-17); and

using the first and second scores to categorize the code under investigation with respect to the likelihood of the code under investigation compromising the security of the computer system (i.e., the system can keep a count of the total weight which is compared against a threshold value)(col. 5, lines 17-21).

Muttik does not explicitly disclose a database of non-malicious code being used by the comparison unit 204.

However, Chess does disclose comparing the code under investigation with the records of database 210 of known non-malicious files/code to determine whether or not the code under investigation matches with any of the known non-malicious files/code in the database 210 (col. 6, lines 5-35).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Muttik with teachings of Chess because it would allow to decide whether the monitored events/code under investigation Is valid/non-malicious by modifying the comparison unit of Muttik to consult with a second database of known non-malicious code as disclosed by Chess. One of ordinary skill in the art would have been motivated by the suggestion of Chess to incorporate a

monitoring program which uses a variety of heuristics to infer that a virus may be present (Chess, col. 1, lines 50-65).

Regarding claims 106 and 116, Muttik discloses wherein the code under investigation has access to other active programs/code executing on the computer system (i.e., code 108 may be introduced into computer system 106 by a remote host 101 across a network 102)(col. 3, lines 30-42).

Regarding claims 107 and 118, Muttik discloses further comprising: selecting, in turn, each additional active program on the computer system as code under investigation, and executing said MCDC with respect to said selected code under investigation (col. 3, lines 23-52).

Regarding claim 129, Muttik discloses further comprising: determining from the score that the code under investigation is malicious code (i.e., weights can be positive for suspicious/malicious activities)(col. 5, lines 15-21).

Regarding claims 132 and 137, Muttik discloses wherein the detection routine examines the behavior of the valid and suspicious code under investigation (col. 3, lines 54-67 and col. 4, lines 1-24 and col. 5, lines 15-21).

Regarding claims 134, 136, 138-139, 141, 143, 145, 148, 150, and 162-166, Muttik discloses determining from the score (i.e., weight) that the code under investigation is malicious code (i.e., weights can be positive for suspicious/malicious activities)(col. 5, lines 15-21).

Regarding claims 135, 142 and 147, Muttik discloses further comprising: determining from the first and second scores that the code under investigation is valid code (i.e., weights can be negative for activities which are more likely to be present in non-malicious code)(col. 5, lines 15-17).

Regarding claims 153-158, Muttik discloses wherein the program instructions are executable to determine whether the first program is a security threat to the computer system based on the first value exceeding a valid code threshold value and the second value exceeding a malicious code threshold value (col. 5, lines 14-21).

Claims 109-114, 130-131, 133, 137, 140, 144, 146, 149, and 160-161 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muttik, (U.S. Patent No. 6,775,780), in view of Chess et al., (U.S. Patent No. 6,772,346 and Chess hereinafter), in further view of Kouznetsov, (U.S. Patent No. 6,973,577).

Regarding claims 109-114, Muttik discloses monitoring suspicious code to detect potentially malicious behavior (col. 3, lines 49-52 and col. 4, lines 25-56).

Chess discloses wherein the malicious code can include computer viruses, worms, or Trojan Horses (col. 3, lines 51-53).

Moreover, Kouznetsov discloses wherein the malicious code includes monitoring software (i.e., events such as system calls having the ability to monitor system input/output activities are monitored)(col. 5, lines 18-67 and col. 6, lines 1-30).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Muttik and Chess with teachings of Kouznetsov because it would include analysis and detection of malicious monitoring software as disclosed by Kouznetsov. One of ordinary skill in the art would have been motivated by the suggestion of Kouznetsov to provide analysis of patterns of behavior characteristic of computer viruses and in case of repetitions of suspicious behavior generating an alert of potential viral activity (Kouznetsov, col. 2, lines 59-63).

Regarding claims 130, 140, 146, 160, and 161, Muttik does not explicitly disclose wherein the malicious code is a previously unknown malicious code.

However, Kouznetsov discloses wherein the malicious code is a previously unknown malicious code (i.e., a knowledge of specific, pre-identified computer viruses would not be necessary because behavioral patterns typical of computer viruses are observed. An example of malicious code with unknown signature is polymorphic viruses)(col. 2, lines 1-2 and lines 21-29).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Muttik and Chess with teachings of Kouznetsov because it would include analysis and detection of malicious monitoring software as disclosed by Kouznetsov. One of ordinary skill in the art would have been motivated by the suggestion of Kouznetsov to provide analysis of patterns of behavior characteristic of computer viruses and in case of repetitions of suspicious behavior generating an alert of potential viral activity (Kouznetsov, col. 2, lines 59-63).

Regarding claim 131, Muttik discloses wherein the detection routine examines the behavior of the suspicious code under investigation (col. 3, lines 49-67 and col. 4, lines 1-24 and col. 5, lines 15-21).

Moreover, Kouzentsov discloses wherein the detection routine examines the behavior of the suspicious code under investigation (i.e., static analyzer 52 performs behavior checking and generates alerts and histograms, wherein "behavior checking" is monitoring the occurrence of an event from the events list and dynamic analyzer 53 analyzes histograms and identifies behavioral repetitions within the histograms which indicate behavior characteristic of a computer virus, wherein such histograms are not know virus signatures associated with any virus)(col. 4, lines 47-67 and col. 5, lines 1-6).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Muttik and Chess

with teachings of Kouznetsov because it would include analysis and detection of malicious monitoring software as disclosed by Kouznetsov. One of ordinary skill in the art would have been motivated by the suggestion of Kouznetsov to provide analysis of patterns of behavior characteristic of computer viruses and in case of repetitions of suspicious behavior generating an alert of potential viral activity (Kouznetsov, col. 2, lines 59-63).

Regarding claim 133, Muttik discloses wherein the detection routine is not specific to the code under investigation (i.e., code 108 is any code that may be introduced into computer system 106 by a remote host 101)(col. 3, lines 23-52).

Moreover, Kouzentsov discloses wherein the detection routine is not specific to the code under investigation (col. 4, lines 15-37).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Muttik and Chess with teachings of Kouznetsov because it would include analysis and detection of malicious monitoring software as disclosed by Kouznetsov. One of ordinary skill in the art would have been motivated by the suggestion of Kouznetsov to provide analysis of patterns of behavior characteristic of computer viruses and in case of repetitions of suspicious behavior generating an alert of potential viral activity (Kouznetsov, col. 2, lines 59-63).

Regarding claims 137, 144, and 149, Muttik discloses further comprising: determining from the score that the code under investigation is suspicious code, wherein suspicious code has not been determined to be either valid or malicious code (col. 3, lines 49-52).

Moreover, Kouzentsov discloses further comprising: determining from the score that the code under investigation is suspicious code, wherein suspicious code has not been determined to be either valid or malicious code (i.e., the categories of the events that are monitored, e.g., events 1-9, col. 5, lines 25-40 may or may not be malicious depending on the repetitions of suspicious behavioral patterns ... the observed group of suspicious events could "potentially" be malicious)(col. 4, lines 38-67 and col. 5, lines 1-67 and col. 6, lines 1-30).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Muttik and Chess with teachings of Kouznetsov because it would include analysis and detection of malicious monitoring software as disclosed by Kouznetsov. One of ordinary skill in the art would have been motivated by the suggestion of Kouznetsov to provide analysis of patterns of behavior characteristic of computer viruses and in case of repetitions of suspicious behavior generating an alert of potential viral activity (Kouznetsov, col. 2, lines 59-63).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AREZOO SHERKAT whose telephone number is (571)272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Arezoo Sherkat/
Patent Examiner
Group 2131
Feb. 25, 2007

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131